Senior Info Security Analyst
Tufts University

Job Title	Senior Info Security Analyst
Department	Technology Services (TTS)
Institution	Tufts University
	Medford, Massachusetts
Date Posted	Nov. 22, 2024
Application Deadline	Open until filled
Position Start Date	Available immediately
Job Categories	Professional Staff
Academic Field(s)	Information Technology
Job Website	https://jobs.tufts.edu/jobs/21171?lang=en-us&iis=Job+Board&iisn=AcademicKeys
Apply By Email	
Job Description	

Overview

Tufts Technology Services (TTS) is a university-wide service organization committed to delivering adaptable, results driven technology solutions in support of Tufts' mission of teaching, learning, research, innovation, and sustainability. With staff working remotely, hybrid and on campus across Tufts University, as well as a 24x7 IT Service Desk, we collaborate with schools and divisions to meet the demands of a global, mobile, and diverse community. We promote a collaborative, forward-thinking, flexible work environment, embrace diversity and inclusion, and encourage personal and professional development.

Senior Info Security Analyst
Tufts University

Fostering a culture of organizational citizenship and making others successful, demonstrating integrity, ethical conduct and optimism, active contribution and continuous learning enables staff to serve the goals and values of the University and creates a fulfilling and positive work experience for all.

What You'll Do

The Senior Information Security Operations Analyst is responsible for leading the implementation and maintenance of information security incident response procedures to protect the university's information assets. This role provides advanced technical support and guidance for security-related issues and collaborates with senior administrators and stakeholders to develop and implement comprehensive security strategies.

- Monitor and analyze security alerts and logs.
- Leads technical incident response efforts, working closely with TTS colleagues to respond to security incidents quickly and effectively.
- Conduct tabletop exercises and simulations to test incident response procedures, identify weaknesses, and enhance the organization's preparedness.
- Mentors other staff on advanced log analysis and security response.
- Take a leading role in organizing phish testing and security awareness training.
- Responsible for evaluating institutional risk of new technology projects by conducting thorough assessments and ensuring that external partners comply with the organization's security standards.
- Tailor the vulnerability management program to more effectively communicate data to stakeholders.
- Assesses technology against the Tufts Security Posture and works with TTS colleagues to implement appropriate security controls to fill gaps in implementation and manage risk.
- Proactively identifies new or important professional working relationships with colleagues and customers. Willing to confront issues and respectfully resolve differences to drive towards a successful conclusion within cross functional teams.
- Regularly provides input on ways to ensure effective and efficient processes with a focus on continuous improvement and performance. Helps team adhere to best practices.
- Commitment to actively enhancing skills and professional development for self and others within the team, follows industry trends, emerging technologies, and best practices and regularly shares knowledge with others.
- Ability to recognize the impact of the changes and analyzes risks and benefits to effectively select and formulate technical solutions.
- Perform tasks on security projects and other duties as assigned.

Schedule Considerations:

- Occasional weekend and evening hours may be required.
- Must be able and willing to participate in a 24x7 on-call rotation for major IT outages and security incidences.
- This position has a work designation of remote.
- Occasional travel to onsite events.

What We're Looking For
Basic Requirements:

- Knowledge and experience typically acquired through a Bachelor's degree plus 6-8 years IT experience
- At least 4 years (concurrent; cumulative with IT experience) that has duties requiring familiarity with a variety of security issues, concepts, practices, and procedures.
- Understanding of networks, IP addresses, and DNS
- Proficient in Windows and Linux configuration and system administration, and troubleshooting experience
- Advanced experience performing security tasks such as: virus cleanup/antivirus management, password or access management, patching, log analysis, firewalls, SPAM, vulnerability scans, VPNs, etc.
- Strong communication skills including writing documentation and presenting to groups
- Working understanding of how compliance such as PCI, Data Privacy, HIPAA, and other regulations affect security, technologies, and processes
- Ability to multi-task and work under stress

Preferred Qualifications:

- Proficiency in scripting languages or code development for task automation
- Familiarity with non-profit or academic environments
- Experience modifying SIEM rules to minimize false positives
- Working knowledge of AWS

Pay Range

Minimum $78,050.00, Midpoint $97,600.00, Maximum $117,150.00

Salary is based on related experience, expertise, and internal equity; generally, new hires can expect pay between the minimum and midpoint of the range.

Contact Information

Please reference Academickeys in your cover letter when applying for or inquiring about this job announcement.

Contact

,